AMENDMENTS TO THE CLAIMS

1. – 71. (Cancelled)

72. (New) A method of dynamically mitigating a noncompliant password, the method comprising:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria;

if the password does not meet the quality criteria, granting to the user a different level of access to the service than if the password meets the quality criteria;

wherein the user is associated with a particular user role, of a plurality of user roles;

wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the particular user role, and wherein a different quality criteria is associated with a second user role of the plurality of user roles;

wherein the quality criteria is based, at least in part, on a strength of the password;

wherein the method is performed by one or more computing devices.

73. (New) The method of Claim 72, further comprising:

if the password meets the quality criteria, granting to the user a first level of access to the service, wherein the granting of the first level of access to the service is dependent on the password exceeding a quality criteria threshold.

74. (New) The method of Claim 72, further comprising:

if the password meets a second quality criteria, granting to the user a second level of access to the service, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

75. (New) The method of Claim 72, further comprising if the password does not meet the quality criteria, performing one or more of:

logging information related to the password;

sending a report about the password;

generating an alert about the password;

forcing a password change; or

blocking the user's access to the service.

76. (New) The method of Claim 72, further comprising providing user access to the service if the password does meet the quality criteria.

77. (New) The method of Claim 72, wherein determining whether the password meets quality criteria further comprises one or more of the steps of:

performing a dictionary look-up based on one or more symbols used in the password;

checking a length of the one or more symbols used in the password;

checking a number of unique characters of the one or more symbols used in the password;

checking a case of the characters in the one or more symbols used in the password;

checking a sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

78. (New) The method of Claim 72, wherein performing one or more responsive actions that relate to accessing the service comprises logging information related to the password.

79. (New) The method of Claim 72, further comprising sending a report about the password if the password does not meet the quality criteria.

80. (New) The method of Claim 72, further comprising generating an alert about the password if the password does not meet the quality criteria.

81. (New) The method of Claim 72, further comprising forcing a password change if the password does not meet the quality criteria.

82. (New) The method of Claim 72, further comprising blocking the user's access to the service if the password does not meet the quality criteria.

83. (New) The method of Claim 72, wherein obtaining the password from the user comprises obtaining the password from the user via a graphical user interface.

84. (New) The method of Claim 72, wherein obtaining the password from the user comprises obtaining the password from the user via an electronic interface.

85. (New) The method of Claim 72, wherein the method further comprises:
determining a quality score for the password, and wherein the step of determining whether the password meets quality criteria comprises comparing the quality score to a predefined threshold value.

86. (New) The method of Claim 72, further comprising:
obtaining the password from a repository of passwords;
making a first determination whether the password meets quality criteria;
storing in a particular machine-readable medium an indication of the first determination for the password;
wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium.

87. (New) The method of Claim 72, wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the service.

88. (New) The method of Claim 72, wherein obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a particular machine, and the service comprises machine executable instructions executing on the same particular machine.

89. (New) The method of Claim 72, wherein obtaining the password comprises an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a first machine and the service comprises machine executable instructions executing on a second machine, wherein the first machine is distinct from the second machine.

90. (New) A method of dynamically mitigating a noncompliant password, the method comprising:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria;

if the password does not meet the quality criteria, granting to the user a different level of access to the service than if the password meets the quality criteria;

wherein the user is associated with a particular user role, of a plurality of user roles;

wherein determining whether the password meets quality criteria comprises

determining whether the password meets quality criteria for the particular user role and wherein a different quality criteria is associated with a second user role of the plurality of user roles;

wherein the quality criteria is based, at least in part, on a strength of the password;

wherein determining whether the password meets quality criteria further comprises

one or more of the steps of:

performing a dictionary look-up based on one or more symbols used in the password;

checking a length of the one or more symbols used in the password;

checking a number of unique characters of the one or more symbols used in the password;

checking a case of the characters in the one or more symbols used in the password;

checking a sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password;

wherein the method is performed by one or more computing devices.

91. (New) The method of Claim 90, further comprising:

if the password meets the quality criteria, granting to the user a first level of access to the service, wherein the granting of the first level of access to the service is dependent on the password exceeding a quality criteria threshold.

92. (New) A non-transitory machine-readable medium storing one or more sequences of instructions for dynamically mitigating a noncompliant password, which instructions, when executed by one or more processors, cause the one or more processors to perform:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria;

if the password does not meet the quality criteria, granting to the user a different level of access to the service than if the password meets the quality criteria;

wherein the user is associated with a particular user role, of a plurality of user roles;

wherein determining whether the password meets quality criteria comprises

determining whether the password meets quality criteria for the particular user role and wherein a different quality criteria is associated with a second user role in the plurality of user roles;

wherein the quality criteria is based, at least in part, on a strength of the password.

93. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform:

if the password meets the quality criteria, granting to the user a first level of access to

the service, wherein the granting of the first level of access to the service is dependent on the password exceeding a quality criteria threshold.

94. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform:

if the password meets a second quality criteria, granting to the user a second level of access to the service, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

95. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: if the password does not meet the quality criteria, performing one or more of:

logging information related to the password;
sending a report about the password;
generating an alert about the password;
forcing a password change; or
blocking the user's access to the service.

96. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: providing user access to the service if the password does meet the quality criteria.

97. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed, cause the one or more processors to perform:
performing a dictionary look-up based on one or more symbols used in the password;
checking a length of the one or more symbols used in the password;
checking a number of unique characters of the one or more symbols used in the

password;

checking a case of the characters in the one or more symbols used in the password;

checking a sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

98. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: logging information related to the password if the password does not meet the quality criteria.

99. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: sending a report about the password if the password does not meet the quality criteria.

100. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: generating an alert about the password if the password does not meet the quality criteria.

101. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: forcing a password change if the password does not meet the quality criteria.

102. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: blocking the user's access to the service if the password does not meet the quality criteria.

103. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: obtaining the password from the user via a graphical user interface.

104. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: obtaining the password from the user via an electronic interface.

105. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: determining a quality score for the password, and wherein determining whether the password meets quality criteria comprises comparing the quality score to a predefined threshold value.

106. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform:
obtaining the password from a repository of passwords;
making a first determination whether the password meets quality criteria;
storing in a particular machine-readable medium an indication of the first determination for the password;
wherein determining whether the password meets quality criteria comprises accessing the particular machine-readable medium.

107. (New) The non-transitory machine-readable medium of Claim 92, further storing instructions which, when executed by the one or more processors, cause the one or more processors to perform: determining whether the password meets quality criteria for the service.

108. (New) An apparatus for dynamically mitigating a noncompliant password, comprising:
one or more processors;
means for obtaining a password from a user when the user attempts to access a service;
means for determining whether the password meets quality criteria;
means for granting a different level of access, if the password does not meet the quality criteria, than if the password meets the quality criteria;
wherein the user is associated with a particular user role, of a plurality of user roles;
wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the particular user role and wherein a different quality criteria is associated with a second user role in the plurality of user roles;
wherein the quality criteria is based, at least in part, on the strength of the password.

109. (New) The apparatus of Claim 108, further comprising:
means for granting a first level of access to the service if the password meets the quality criteria, wherein the first level of access to the service is associated with the quality criteria.

110. (New) The apparatus of Claim 108, further comprising:
means for granting to the user a second level of access to the service, if the password meets a second quality criteria, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

111. (New) The apparatus of Claim 108, further comprising means for performing, if the password does not meet the quality criteria, one or more of:
means for logging information related to the password;
means for sending a report about the password;

means for generating an alert about the password;
means for forcing a password change; or
means for blocking the user's access to the service.

112. (New) The apparatus of Claim 108, wherein the apparatus further comprises means for providing user access to the service if the password does meet the quality criteria.

113. (New) The apparatus of Claim 108, wherein the means for determining whether the password meets quality criteria further comprises one or more of:
means for performing a dictionary look-up based on one or more symbols used in the password;
means for checking a length of the one or more symbols used in the password;
means for checking a number of unique characters of the one or more symbols used in the password;
means for checking a case of the characters in the one or more symbols used in the password;
means for checking a sequencing of characters in the one or more symbols used in the password; or
means for performing statistical analysis based on the one or more symbols used in the password.

114. (New) The apparatus of Claim 108, further comprising means for logging information related to the password if the password does not meet the quality criteria.

115. (New) The apparatus of Claim 108, further comprising means for sending a report about the password if the password does not meet the quality criteria.

116. (New) The apparatus of Claim 108, further comprising means for generating an alert about the password if the password does not meet the quality criteria.

117. (New) The apparatus of Claim 108, further comprising means for forcing a password change if the password does not meet the quality criteria.

118. (New) The apparatus of Claim 108, further comprising means for blocking the user's access to the service if the password does not meet the quality criteria.

119. (New) The apparatus of Claim 108, wherein the means for obtaining the password from the user comprises means for obtaining the password from the user via a graphical user interface.

120. (New) The apparatus of Claim 108, wherein the means for obtaining the password from the user comprises means for obtaining the password from the user via an electronic interface.

121. (New) The apparatus of Claim 108, wherein the apparatus further comprises means for determining a quality score for the password, and wherein the means for determining whether the password meets quality criteria comprises means for comparing the quality score to a predefined threshold value.

122. (New) The apparatus of Claim 108, further comprising:
means for obtaining the password from a repository of passwords;
means for making a first determination whether the password meets quality criteria;
means for storing in a particular machine-readable medium an indication of the first determination for the password;
wherein the means for determining whether the password meets quality criteria comprises means for accessing the particular machine-readable medium.

123. (New) The apparatus of Claim 108, wherein means for determining whether the password meets quality criteria comprises means for determining whether the password meets quality criteria for the service.

124. (New) The apparatus of Claim 108, wherein the means for obtaining the password comprises means for an access service to obtain the password from the user when the user attempts to access the service, and wherein the access service comprises means for executing on a particular machine, and wherein the service comprises means for executing on the same particular machine.

125. (New) The apparatus of Claim 108, wherein the means for obtaining the password comprises means for an access service to obtain the password from the user when the user attempts to access the service, and wherein the access service comprises means for executing on a first machine and the service comprises means for executing on a second machine, wherein the first machine is distinct from the second machine.

126. (New) An apparatus for dynamically mitigating a noncompliant password, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform:

obtaining a password from a user when the user attempts to access a service;

determining whether the password meets quality criteria;

if the password does not meet the quality criteria, granting to the user a different level of access to the service than if the password meets the quality criteria;

wherein the user is associated with a particular user role, of a plurality of user roles;

wherein determining whether the password meets quality criteria comprises determining whether the password meets quality criteria for the particular user role and wherein a different quality criteria is associated with a second user role in the plurality of user roles;

wherein the quality criteria is based, at least in part, on a strength of the password.

127. (New) The apparatus of Claim 126, further comprising instructions which, when executed by the processor, cause the processor to perform: if the password meets the quality criteria, granting to the user a first level of access to the service, wherein the granting of the first level of access to the service is dependent on the password exceeding a quality criteria threshold.

128. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: if the password meets a second quality criteria, granting to the user a second level of access to the service, wherein the second level of access to the service is associated with the second quality criteria, wherein the second quality criteria is distinct from the quality criteria and wherein, if a particular password meets the quality criteria, then the password meets the second quality criteria.

129. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: if the password does not meet the quality criteria, performing one or more of:

logging information related to the password;
sending a report about the password;
generating an alert about the password;
forcing a password change; or
blocking the user's access to the service.

130. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: providing user access to the service if the password does meet the quality criteria.

131. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform:

performing a dictionary look-up based on a one or more symbols used in the password;

checking a length of the one or more symbols used in the password;

checking a number of unique characters of the one or more symbols used in the password;

checking a case of the characters in the one or more symbols used in the password;

checking a sequencing of characters in the one or more symbols used in the password; or

performing statistical analysis based on the one or more symbols used in the password.

132. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: logging information related to the password if the password does not meet the quality criteria.

133. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: sending a report about the password if the password does not meet the quality criteria.

134. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: generating an alert about the password if the password does not meet the quality criteria.

135. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: forcing a password change if the password does not meet the quality criteria.

136. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: blocking the user's access to the service if the password does not meet the quality criteria.

137. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: obtaining the password from the user via a graphical user interface.

138. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: obtaining the password from the user via an electronic interface.

139. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform:: determining a quality score for the password, and wherein determining whether the password meets quality criteria comprises comparing the quality score to a predefined threshold value.

140. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform:
obtaining the password from a repository of passwords;
making a first determination whether the password meets quality criteria;
storing in a particular machine-readable medium an indication of the first determination for the password;
wherein the step of determining whether the password meets quality criteria comprises accessing the particular machine-readable medium.

141. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to

perform: determining whether the password meets quality criteria for the service.

142. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on the apparatus, and the service comprises machine executable instruction executing on the same apparatus.

143. (New) The apparatus of Claim 126, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform: an access service obtaining the password from the user when the user attempts to access the service, and wherein the access service comprises machine executable instructions executing on a first machine and the service comprises machine executable instructions executing on a second machine, wherein the first machine is distinct from the second machine.